Identity Theft Protection

Keep Your Identity Safe

- Consider freezing your credit with the 3 major credit bureaus – Equifax, Experian and Transunion
- Request a copy of your credit report on an annual basis and review it – it's free!
- Set up fraud alerts on all of your financial accounts
- File your taxes as soon as possible to avoid having a fraudster do it on your behalf
- Shred all documents containing personal and financial information

Home Device Security

Protect Your Home Devices

- Change default usernames and passwords on devices
- Check privacy and data sharing options on the device
- Secure the device account with a long and strong password
- Consider connecting your IoT devices to a separate Wi-Fi network
- Allow your device to install automatic updates

Maintain Your Computer System

Look Closer To Avoid Malware

- Be skeptical when receiving random pop-ups or error messages appearing to be from an antivirus software that you do not even have installed on your device
- Use antivirus software and always keep it updated
- Only download software from known and trusted websites and companies
- Configure your antivirus to run daily automated scans

Stay Protected on the Go

Defend Your Mobile Security

- Do not store personal information on your mobile device (SSNs, account numbers, etc.)
- Consider using a remote lock or wipe service in the event your device is lost or stolen
- Turn off unused features if you don't need them on (Bluetooth, Wi-Fi, NFC, etc.)
- Only download apps from Google and Apple Play stores
- Monitor permission access/ request from apps
- Lock your device with either a password, pin or biometric

Reinforce Security Online

Keep Your Password Strong

- Never write down your passwords and keep them in an unsecured manner (sticky-notes on your desk) or share them with others
- When possible, use multi-factor authentication
- Longer is stronger – consider using a passphrase for a password
- Never reuse your passwords – they should be unique for every account
- Consider using a password manager to securely store and create passwords

Stay Away from Phishy Emails

Don't Get Hooked By Phishers

- Never respond to emails requesting personal information and/or account details
- Don't click on embedded links or open attachments without first examining the email
- Hover your mouse cursor over a link to see the web address of where the link would take you
- Inspect the email for any odd language, poor grammar or misspellings
- Inspect the sender's email address to ensure it's valid, however use caution – email addresses can be spoofed to appear legitimate

Keep Track of What's Important

Secure Sensitive Information

- Shred all documents with personal and confidential information
- Do not share or leave out your ID where someone can grab it
- Lock your computer screen when unattended
- Beware of someone trying to tailgate you into the building or restricted area
- Prevent shoulder surfing – be aware of your surroundings
- Do not use or plugin unknown storage media devices

Practice Safe Web Browsing

Be Careful When Your Browse

- Look for "https" in the address bar preceded by a small padlock symbol to ensure a secure encrypted session and that the site has a valid certificate
- Be cautious logging into websites or entering personal information while using public Wi-Fi
- Watch out for advertisements that appear too good to be true – they could be malicious
- Consider using a VPN when connected to a public Wi-Fi network
- Go directly through a website rather than clicking on a link
- Do not use or plugin unknown storage media devices

Social Media Smart Practices

Keep Your Identity Safe

- Think before you click on links to articles, videos or advertisements that people share
- Be discreet – avoid posting too much personal information
- Familiarize yourself with the privacy settings for your social media account
- Consider protecting your social media account with multi-factor authentication
- Be aware of fake friend requests – do not accept duplicate friend requests

See Something Say Something

Report Anything Suspicious

- Report suspicious or unauthorized network activity, system use or violation of mobile computing rules
- Report strange emails or suspected phishing attempts
- Report theft or loss of any electronic storage devices
- Report any breach, compromise or corruption of information
- Report unexpected security tests, system disruptions or failure

Stay Safe When You Connect

Be Aware, Connect With Care

- Consider using a personal hotspot device (Mi-Fi) or trusted device as a hotspot instead of relying on public Wi-Fi
- Protect your Wi-Fi network using WPA2/WPA3 connections
- If unsure what Wi-Fi network to connect to, ask for confirmation
- When possible stick to known and trusted Wi-Fi networks
- Avoid logging into personal accounts on public Wi-Fi (email, social media, bank accounts, etc.)
- Secure your own Wi-Fi network and router with a strong password
- Update your router firmware for any new security patches

GreyCastle SECURITY

Multi-Factor Authentication

Don't Let Anyone Sign-In As You

- Apps, like Duo, can help you set up multi-factor authentication for each of your sign-ins
- Implementing multi-factor authentication is often a key requirement for achieving compliance with data protection laws and regulations
- Securely sign in to an application or website by setting up a one-time password to be delivered via a smartphone app or SMS message
- Reduce password fatigue by implementing multi-factor authentication and a password manager
- Protect against credential theft by ensuring that a password login isn't enough to authenticate a login attempt

GreyCastle SECURITY